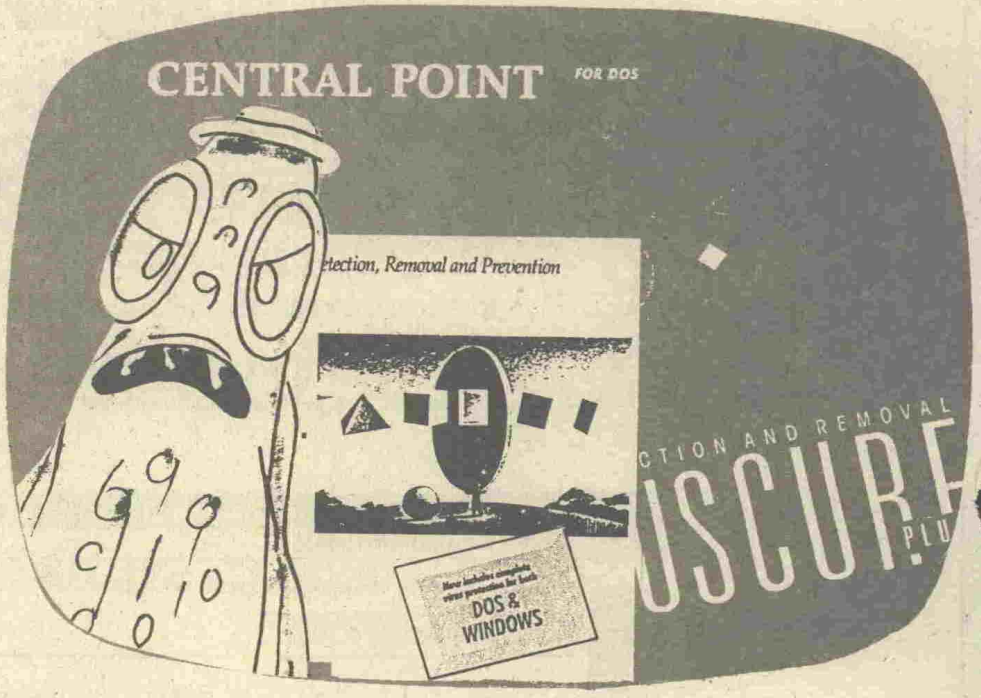
สรัญญา ธรรมพิทักษ์

พิชิตศึก! ด้วย แอนตี้ไวรัส

ประกาศศักดาแห่งความสามารถในการทำงานของโปรแกรมแอนตี้ไวรัสที่ลือชื่อ



มื่อกล่าวถึงไวรัสคอมพิวเตอร์แล้ว นักคอมพิวเตอร์ทั้งหลายคงจะรู้จักและคุ้นเคยกันเป็นอย่างดี เนื่องจากเจ้าไวรัสคอมพิวเตอร์ได้เข้ามาคุกคามและทำอันตรายให้กับข้อมูลซึ่งก่อให้เกิดความเสียหายแก่วงการคอมพิวเตอร์ของเมืองไทยเป็นอย่างมาก ไวรัสคอมพิวเตอร์ได้เข้ามาเยี่ยมเยือนประเทศไทยเมื่อปี พ.ศ. ใดก็ไม่อาจจะทราบได้ แต่เมื่อกลางปี พ.ศ. 2531 เจ้าไวรัสก็ได้ก่อความวุ่นวายและแพร่กระจายไปเต็มเมืองแล้ว จนถึงในปัจจุบันนี้ไวรัสคอมพิวเตอร์ก็ได้เพิ่มจำนวนขึ้นเรื่อย ๆ ดังนั้นในบทความเรื่องนี้จะนำท่านผู้อ่านไปพบกับ การเปรียบเทียบประสิทธิภาพของโปรแกรมกำจัดไวรัสกัน เราสามารถทำการวิเคราะห์การทำงานของไวรัสคอมพิวเตอร์ได้ 3 ลักษณะ

1. เป็นพาหะ จะเป็นช่วงที่ทำการแพร่เชื้อไวรัส จากตัวมันเองไปสู่ไฟล์ตัวอื่น ๆ โดยการคัดลอกโปรแกรมไวรัสไปยังแฟ้มข้อมูลอื่น ๆ ที่มีอยู่ในระบบ แต่ยังไม่ทำอันตรายข้อมูลเหล่านั้น เพียงแต่จะคัดลอกไปเรื่อย ๆ

2. ทำลายเมื่อถูกกระตุ้น การทำงานในลักษณะนี้คล้ายกับการวางระเบิดเวลา ถ้าถึงเวลาที่กำหนดไว้ไวรัสก็จะออกมาทำลายข้อมูลทันที แล้วจะหยุดไปจนกว่าจะครบกำหนดเวลาอีกครั้งก็จะออกมาทำลายอีก ซึ่งจะเป็นลักษณะนี้ไปเรื่อย ๆ เช่น ไวรัสศุกร์ที่ 13 (Friday 13 th) และไวรัสคริสต์มาส (Christmas Virus)

3. ปฏิบัติการและทำลาย การทำงานของโปรแกรมไวรัสชนิดนี้ เป็นลักษณะการทำงานที่โหดที่สุด เนื่องจากว่าถ้ามีไวรัสชนิดนี้เข้าไปในระบบงานข้อมูลในระบบงานก็จะถูกทำลายทันที เช่น ถูกลบข้อมูลบางส่วนออกจากไฟล์ หรือคัดลอกส่วนหนึ่งของโปรแกรมใดโปรแกรมหนึ่งไปยังอีกส่วนหนึ่งของอีกโปรแกรมหนึ่ง ทำให้โปรแกรมหรือข้อมูลเกิดความผิดพลาดและอาจจะถูกทำลายในที่สุด

นอกจากนี้แล้วยังสามารถแบ่งประเภทในการติดเชื้อของไวรัสได้เป็น 8 ประเภทใหญ่ ๆ

1. พวกที่ฝังตัวอยู่ในบูตเซกเตอร์ เป็นไวรัสที่ฝังตัวอยู่ในส่วนของบูตเซกเตอร์ในแผ่นดิสก์ ซึ่งเป็นบริเวณที่เครื่องต้องทำการโหลดส่วนนี้ลงในหน่วยความจำหลังจากทำการเปิดเครื่องเสมอ ทำให้โปรแกรมไวรัสชนิดนี้ได้

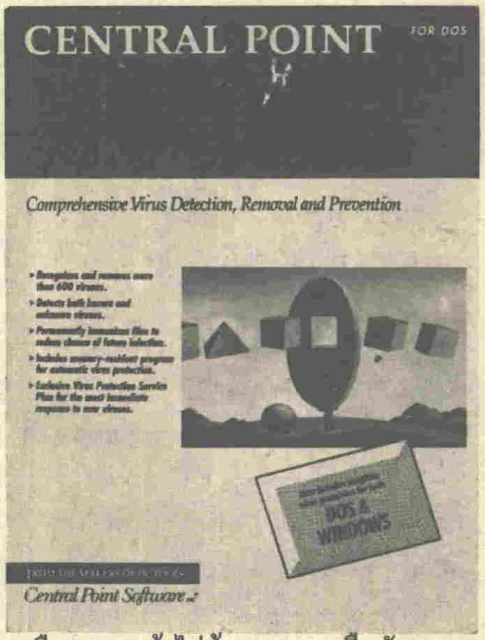
ปฏิบัติการแพร่พันธุ์ถูกหลานเข้าไปตามไฟล์โปรแกรมต่าง ๆ ที่ถูกเรียกใช้ และเมื่อถึงเวลาอันสมควรมันก็จะออกอาละวาดทันที

2. พวกที่ฝังตัวใน command.com โดยปกติแล้ว command.com เป็นโปรแกรมที่ทำหน้าที่อำนวยความสะดวกให้ผู้ใช้สามารถติดต่อและสั่งงานกับเครื่องคอมพิวเตอร์ได้ ด้วยภาระหน้าที่เช่นนี้ทำให้ command.com ถูกเรียกใช้ตลอดเวลา จึงก่อให้เกิดอันตรายต่อระบบการทำงานของโปรแกรมเป็นอย่างมาก เนื่องจากการโหลดโปรแกรมบ่อยครั้งทำให้ไวรัสลงสู่หน่วยความจำมากขึ้น และพร้อมที่จะปฏิบัติการทำลายล้างข้อมูลตามระยะเวลาที่เหมาะสม

3. พวกที่ติดลงไปบนโปรแกรมประยุกต์ที่มีนามสกุล (Extention) เป็น .COM, .EXE, .BIN, .SYS และไฟล์โอเวอร์เลย์ โปรแกรมไวรัสประเภทนี้เป็นโปรแกรมไวรัสที่มีมากที่สุด และสามารถแพร่กระจายได้อย่างรวดเร็ว เนื่องจากไฟล์เหล่านั้นสามารถที่จะเอ็กซีคิวต์ (execute) จาก Dos Promt ได้ ทำให้มันฝังตัวในหน่วยความจำ เมื่อผู้ใช้เรียกใช้งานในโปรแกรมอื่นต่อไป มันก็จะเข้าไปติดเชื้อในโปรแกรมนั้นทันที

4. พวกที่ติดลงไปในส่วนพาร์ติชันของฮาร์ดดิสก์ เป็นส่วนที่ใช้ในการเก็บข้อมูลในฮาร์ดดิสก์ ซึ่งเป็นส่วนสำคัญมากและยังเป็นส่วนที่ไวรัสจะเข้าไปทำลาย ดังนั้นถ้าไวรัสเข้าไปในส่วนนี้ก็จะทำให้ฮาร์ดดิสก์ไม่สามารถเรียกใช้งานได้ และข้อมูลต่าง ๆ ที่อยู่ในฮาร์ดดิสก์ก็ไม่สามารถเรียกใช้งานได้เช่นกัน

5. ในส่วนของ FAT (file allocation table) ลักษณะการทำงานของโปรแกรมไวรัสชนิดนี้ เมื่อเข้าไปในส่วนของ FAT มันจะเข้าไปทำลาย FAT



หรืออาจจะเข้าไปย้าย FAT หรือคัดลอกตัวของมันเองทับไปในส่วนของ FAT ทำให้ไม่สามารถเรียกใช้งานในโปรแกรมต่าง ๆ เหล่านั้นได้

6. พวกที่เป็นพันธุ์ผสมคือ สามารถทำงานได้ทั้งข้อ 1, 2, 3 เป็นไวรัสที่มีคุณสมบัติพิเศษ มันสามารถทำงานได้ทั้ง 3 ลักษณะ และเป็นโปรแกรมไวรัสที่สามารถปฏิบัติการก่อกวนระบบการทำงานของคอมพิวเตอร์ประสบผลสำเร็จมากที่สุดในขณะนี้

7. พวกที่ติดเฉพาะไฟล์ เป็นไวรัสที่จะทำลายเฉพาะไฟล์ที่ต้องการเท่านั้น และจะต้องเริ่มปฏิบัติการทำลายเมื่อถึงระยะเวลาที่สมควร

8. พวกที่ฝังตัวในหน่วยความจำ ประเภทของไวรัสที่กล่าวมาแล้วอาจจะมีคุณสมบัติเช่นนี้รวมอยู่ด้วย ไวรัสชนิดนี้เมื่อฝังตัวลงไปในหน่วยความจำแล้ว มันจะเริ่มปฏิบัติการทำงานไปตามชุดคำสั่งที่กำหนดไว้ จนกระทั่งถึงสถานการณ์ที่ได้กำหนดมาในโปรแกรม โปรแกรมไวรัสมันก็จะออกอาละวาดทันที เช่น มีเสียงเพลงดังขึ้น, คีย์บอร์ดค้าง, หน้าจอมีขยะขึ้นมา เป็นต้น

แนะนำแอนตี้ไวรัส

ไวรัสคอมพิวเตอร์ได้เกิดขึ้นมาเนื่องจากความบ้าบิ่นของโปรแกรมเมอร์ทั้งหลายที่ต้องการแสดงฝีไม้ลายมือให้เห็นกัน โดยไม่คำนึงถึงความเสียหายที่เกิดขึ้น ถึงอย่างไรก็ตาม เมื่อมีผู้สร้างก็ต้องมีผู้ทำลาย ซึ่งในปัจจุบันนี้ได้มีโปรแกรมสำหรับทำการปราบและกำจัดไวรัสขึ้นมามากมาย ซึ่งแต่ละตัวก็จะมีประสิทธิภาพการทำงานที่แตกต่างกันออกไป ในบทความต่อไปจะทำการเปรียบเทียบประสิทธิภาพการทำงานของโปรแกรมกำจัดไวรัส โดยได้ทำการคัดเลือกโปรแกรมกำจัดไวรัสมาทั้งหมด 5 ชุด คือ

1. VIRUSCURE PLUS
2. VIREX-PC
3. SCAN V.82
4. CPAV (CENTRAL POINT ANTIES VIRUS)
5. NAV (NORTON ANTIES VIRUS)

ลักษณะการทำงานของโปรแกรมทั้ง 5 ชุดนี้ พอจะสรุปลักษณะการทำงานได้ 3 ลักษณะคือ

1. VIRUS DETECTION

เป็นลักษณะการทำงานของโปรแกรมที่ใช้ในการตรวจสอบไวรัส ซึ่งจะใช้วิธีในการคำนวณหาค่าผลรวมของพื้นที่ในไฟล์ (เรียกว่าการ CHECKSUM) และเก็บค่าผลรวมเอาไว้ จะถูกนำมาใช้เพื่อเปรียบเทียบเมื่อมีการเรียกใช้ไฟล์โปรแกรมดังนี้ ถ้าค่าผลรวมที่ได้แตกต่างกัน แสดงว่าไฟล์นั้นมีอาการผิดปกติ อาจจะติดไวรัส โปรแกรมก็จะทำการตรวจสอบว่าความผิดปกตินั้นเกิดขึ้นจากไวรัสชนิดใด ถ้าเป็นไวรัสที่โปรแกรม

นั้นรู้จักก็จะแจ้งชื่อให้ทราบ แต่ถ้าไม่รู้จักโปรแกรมก็จะแจ้งให้ทราบถึงความผิดปกติที่เกิดขึ้นว่าเกิดตรงตำแหน่งและไฟล์ใด

2. VIRUS PROTECTION

การทำงานของโปรแกรมนี้จะทำการตรวจสอบการทำงานของระบบตลอดเวลา โปรแกรมในลักษณะนี้ส่วนมากจะเป็นโปรแกรมเรสซิเดนต์ การทำงานของโปรแกรมชนิดนี้จะเข้าไปทำงานในส่วนที่สำคัญที่ไวรัสเข้าไปรุกราน เมื่อเข้าไปทำการตรวจสอบแล้วได้พบว่า กำลังจะเกิดสิ่งผิดปกติบริเวณนั้น ก็จะทำการร้องเตือนผู้ใช้ทราบทันที และจะแนะนำวิธีการแก้ไขให้ผู้ใช้ตัดสินใจว่าจะทำอย่างไรต่อไป

3. VIRUS REMOVAL

การทำงานของโปรแกรมประเภทนี้จะใช้วิธีการค้นหาลักษณะเฉพาะของไวรัสแต่ละตัว ซึ่งตัวโปรแกรมจะรู้จักไวรัสเหล่านั้น แต่ถ้าเป็นไวรัสที่เกิดขึ้นมาใหม่ก็ไม่สามารถจะทำการตรวจสอบและค้นหาไวรัสได้ ดังนั้นโปรแกรมที่ทำงานในลักษณะนี้เหมาะที่จะใช้ในการตรวจสอบซอฟต์แวร์ตัวใหม่ว่ามีไวรัสตัวไหนบ้าง นอกจากนี้แล้วการทำงานของโปรแกรมในลักษณะนี้ยังสามารถที่จะช่วยดึงเอาไวรัสที่ติดลงไปในส่วนไฟล์ต่าง ๆ ออกมา และไฟล์เหล่านั้นก็สามารถที่จะทำงานได้ตามปกติ แต่จะมีบางไฟล์เท่านั้นที่ไม่สามารถทำงานต่อไปได้

เปิดฉากแอนตี้ไวรัส

VIRUSCURE PLUS

VirusCure Plus เป็นโปรแกรมแอนตี้ไวรัสที่ใช้ในการตรวจสอบและช่วยในการ protect ไวรัสได้มากกว่า 230 ชนิด และยังสามารถ detect ไวรัสที่ไม่รู้จักได้อีกด้วย ในจำนวนไวรัสเหล่านั้นได้รวมถึงไวรัสดังต่อไปนี้ด้วย

The Alabama Virus เป็นไวรัสที่เข้าไปทำลาย FAT (File Allocation Table) ของข้อมูล ทำให้ข้อมูลไม่สามารถอ่านได้

The Dark Avenger เป็นไวรัสที่เข้าไปบันทึกทับเซกเตอร์ในดิสเกตต์หรือฮาร์ดดิสก์และเข้าไปทำลายข้อมูลเหล่านั้น

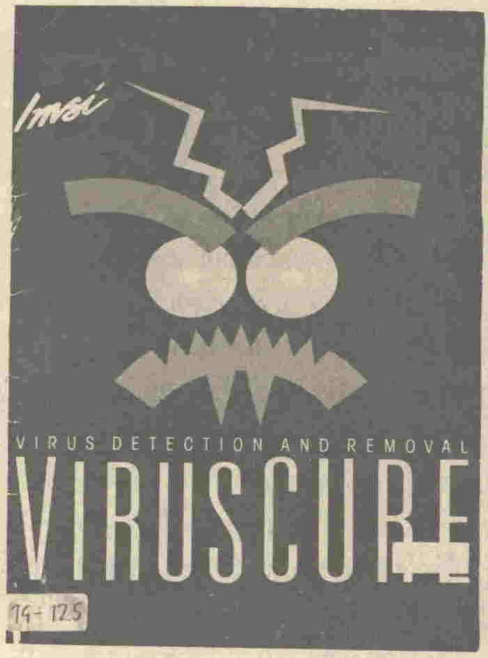
The Christmas Virus เป็นไวรัสที่เข้าไปทำลายข้อมูลในตารางพาร์ติชันของฮาร์ดดิสก์ โดยจะเริ่มการทำงานในวันที่ 1 เมษายน ของปีนั้น ๆ เมื่อถึงวันที่ 24 ธันวาคม ไปจนกระทั่งถึงวันที่ 1 มกราคม ไวรัสตัวนี้จะร่วมฉลองคริสต์มาสด้วย โดยการแสดงรูปต้นคริสต์มาสไว้บนจอภาพ

The Disk Killer ไวรัสตัวนี้เมื่อติดเข้าไปแล้ว จะเข้าไปทำลายดิสเกตต์ทั้งแผ่น โดยจะทำการ reformat แผ่นดิสเกตต์เหล่านั้น

The Jurusalem Virus เป็นโปรแกรมไวรัสที่ฝังตัวลงไปในแผ่นดิสเกตต์จนกระทั่งถึงวันศุกร์ที่ 13 จะเข้าไปลบโปรแกรมทุกโปรแกรมที่ทำงานในวันนั้น

คุณสมบัติทั่วไป

- สามารถ detect ไวรัสได้เกือบทุกชนิด
- ช่วยป้องกันไวรัสทั้งที่รู้จักและไม่รู้จัก พร้อมทั้งทำการฉีดวัคซีนเพื่อป้องกันไม่ให้ไวรัสเข้าไปติดไฟล์ในระบบ
- ช่วยทำลายไวรัสบางตัวที่เข้าไปติดไฟล์ในแผ่นโดยไม่ทำอันตรายให้กับไฟล์
- ช่วยสร้างภูมิคุ้มกันให้กับไฟล์ข้อมูลที่เคยติดไวรัส
- ในการตรวจค้นหาไวรัส จะทำการตรวจหา Signature ของไฟล์ โดยจะตรวจสอบในส่วนของ DOS, BIOS, Boot Sector, Partition table หรือส่วนอื่น ๆ ในกรณีที่มีความผิดปกติขึ้นตรงส่วนนั้น



เมื่อทำการรันโปรแกรม VirusCure Plus โปรแกรมจะทำการสแกนหาไวรัสจากระบบและแผ่นดิสเกตต์ ถ้าพบไวรัสที่รู้จักและสามารถทำลายได้ก็จะทำลายในทันที และจะฉีดวัคซีนป้องกันไฟล์นั้นไม่ให้ติดไวรัสอีก โปรแกรม VirusCure Plus จะทำงานเป็นเรสซิเดนต์โปรแกรม ใช้เนื้อที่บนหน่วยความจำเพียง 25 กิโลไบต์ VirusCure Plus ยังเปิดโอกาสให้คุณทำการแก้ไขและเพิ่มเติมคุณสมบัติบางอย่างที่ต้องการลงไปในไฟล์ CURE.EXE โดยทำการรันจาก DOS PROMT ในการรันโปรแกรม VirusCure Plus สามารถทำการรันได้หลายวิธี แต่เพื่อความสะดวกในการทำงานและสามารถทำงานได้ทันทีเมื่อทำการเปิดเครื่อง โดยทำการเซตค่าต่าง ๆ ไว้ใน AUTOEXEC.BAT

ก่อนติดตั้งโปรแกรม

ก่อนทำการติดตั้งโปรแกรม จะต้องทำการค้นหาไวรัสในระบบเสียก่อน โดยใช้โปรแกรม CURE.EXE ซึ่งโปรแกรมตัวนี้จะอยู่ในแผ่นโปรแกรม Virus-Cure Plus เป็นโปรแกรมที่ช่วยในการตรวจสอบ

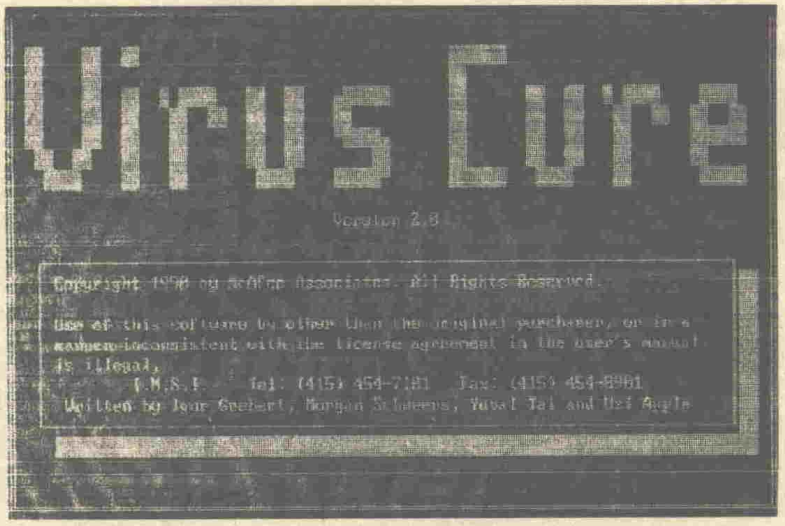
```
A> cure <Enter>
```

ที่หน้าจอจะแสดงไตเติ้ล ดังรูปที่ 1 ให้กด Enter อีกครั้งหนึ่ง จะได้ดังรูปที่ 2 หลังจากนั้นโปรแกรมจะทำการตรวจสอบในส่วนต่าง ๆ ที่สำคัญ คือ Bootsector, Partition table, Operating System file และ Overlays file ถ้าไม่พบไวรัสก็สามารถติดตั้งโปรแกรมในระบบได้เลย (ถ้าต้องการตั้งค่า Configuration ของโปรแกรมใหม่ให้กด F10 จะแสดงดังรูปที่ 3) แต่ถ้าพบว่ามีไวรัสอยู่ในระบบ โปรแกรม VirusCure plus จะมีออปชัน. ให้เลือกคือ

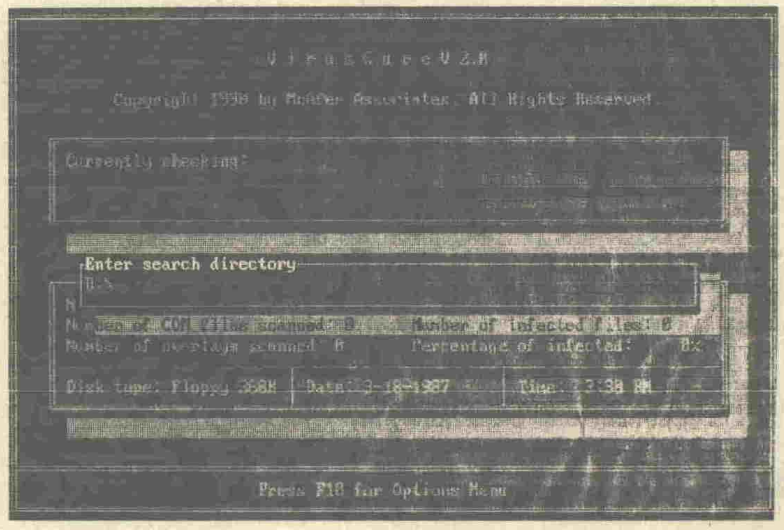
```
- removing the virus
- terminainy the scan
```

ถ้าเลือก removal โปรแกรมจะทำลายไวรัสที่ติดไปในไฟล์นั้น และแก้ไขไฟล์นั้นให้ใช้งานได้ แต่ในบางครั้งอาจจะใช้งานไม่ได้เพราะไวรัสได้ทำลายบางส่วนของไฟล์ไปแล้ว แต่ถ้าโปรแกรมไม่สามารถแก้ไขไฟล์ใช้งานได้ หรือไม่สามารถทำลายไวรัสในส่วนนั้นได้ จะแสดงข้อความว่าต้องการจะลบไฟล์ที่ติดไวรัสออกไปหรือไม่ ถ้าต้องการลบให้ตอบ YES โปรแกรมก็จะทำการลบไฟล์ที่ติดไวรัสออกไป ถ้าเลือก terminate โปรแกรมจะหยุดการทำงานออกไปสู่ DOS

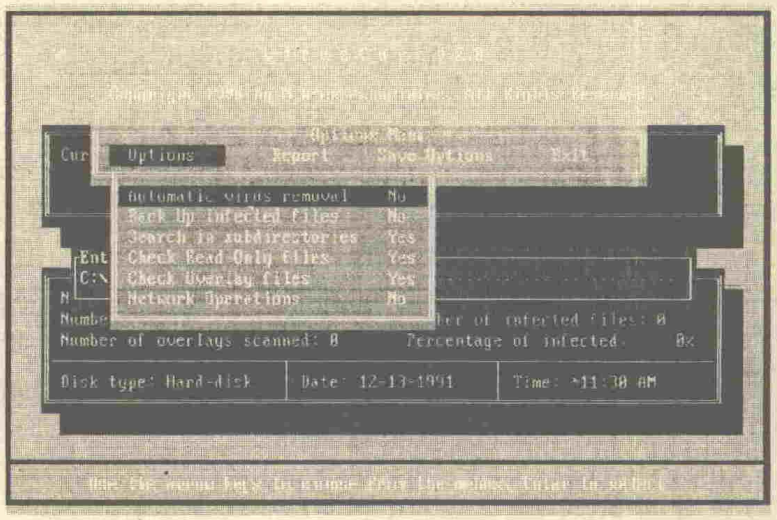
คุณสามารถทำงานกับโปรแกรม VirusCure Plus ได้มากขึ้นโดยการใช้ค่าพารามิเตอร์ต่าง ๆ ดังนี้



รูปที่ 1 แสดงไตเติ้ลของโปรแกรม Virus Cure Plus



รูปที่ 2



รูปที่ 3 แสดงเมนูในการทำงานของโปรแกรม

a: ถ้าพบไวรัสในระบบให้ทำลายได้ทันที
b: สร้างไฟล์สำรอง (Backup Data) ไว้อีกชุดหนึ่ง
d: รันขณะที่ทำงานเป็น Direct mode
h: Help menu
m: รันบนจอโมโนโครม
n: รันในระบบ LAN
o: ตรวจสอบ overlay ของไฟล์
r: ตรวจสอบในส่วนที่เป็น read-only
s: ตรวจสอบซับไดเรคทอรี

ตัวอย่างเช่น

```
A:> cure / d C:
A:> cure /d C: D: E: \ BIN E: \ WORD
A:> cure /m
```

ติดตั้งโปรแกรม

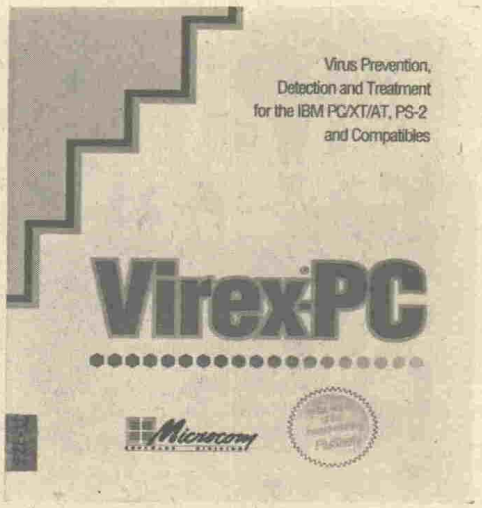
หลังจากที่ทำการรันโปรแกรม VirusCure Plus แล้ว และพบว่าภายในระบบคอมพิวเตอร์ของคุณปราศจากไวรัส ก็สามารถทำการติดตั้งโปรแกรม VirusCure Plus ได้ดังนี้

```
A> INSTALL <ENTER>
```

บนจอภาพจะแสดงข้อความต่าง ๆ ที่เกี่ยวกับ VirusCure Plus ให้กด Enter อีกครั้งหนึ่งจะมีคำแนะนำเกี่ยวกับวิธีใช้โปรแกรมแสดงบนจอภาพ ถ้าต้องการออกจากคำแนะนำนั้นให้กด ESC โปรแกรมจะทำการโหลดไฟล์ข้อมูลต่าง ๆ ออกมาแสดงบนเมนู ซึ่งจะมีออปชันให้เลือกแสดงบนจอภาพดังรูปที่ 4

- Install VirusCure Plus (tm) on hard disk
- De-Install VirusCure Plus (tm) FROM disk
- Reconstruction of boot partition
- Exit

รูปที่ 4 แสดงออปชันให้เลือกในขณะทำการติดตั้ง



ให้เลือกออปชันแรกเพื่อทำการติดตั้งโปรแกรมลงฮาร์ดดิสก์ เมื่อทำการติดตั้งโปรแกรมลงฮาร์ดดิสก์แล้วก็สามารถใช้โปรแกรม VirusCure Plus ได้

ของฝาก

โปรแกรม VirusCure Plus เป็นโปรแกรมที่เรสซิเดนต์ในหน่วยความจำ ซึ่งจะใช้เนื้อที่ในหน่วยความจำ 25 กิโลไบต์ สามารถทำการรันใช้งานในระบบ LAN ได้โดยใช้คำสั่ง

```
A> cure /n
```

ในกรณีที่ไม่ต้องการใช้งาน VirusCure Plus สามารถทำการ de-install โปรแกรมออกจากระบบงานได้

VIRUSCAN82 หรือ SCAN82

โปรแกรม VIRUSCAN82 นับเป็นโปรแกรมที่ต้องพัฒนาตลอดเวลา (เนื่องจากเป็นโปรแกรมไวรัสชนิดที่เรียกว่า detection) จนถึงปัจจุบันก็คือ SCAN 7.8V82 ซึ่งสามารถตรวจหาไวรัสได้ทั้งหมด 297 พันธุ์หรือ 893 ตัวที่มีอยู่ในโลก ถ้าคิดเป็นเปอร์เซ็นต์แล้วสูงถึง 98% ของไวรัสที่มีอยู่

หลักการทำงานโดยทั่วไปขอ
VIRUSCAN82 คือการเก็บข้อมูลต่าง
ของไวรัสคอมพิวเตอร์ที่มีอยู่พร้อมกั
เก็บชื่อของไวรัสแต่ละชนิดด้วยเพื่อใ
ในการค้นหาไวรัส ถ้าพบว่าโปรแกร
ที่ใช้ VIRUSCAN82 ตรวจเช็คอยู่
ข้อมูลตรงกับข้อมูลไวรัสที่เก็บไว้ก็จะแจ้
ให้ทราบ จึงทำให้โปรแกรม VIRU
SCAN82 ต้องถูกอัพเดตอยู่ตลอดเวล
เพื่อให้โปรแกรมมีความทันสมัยขึ้น

ทำความรู้จัก VIRUSCAN82

VIRUSCAN82 สามารถทำงานบ
พีซีที่มีหน่วยความจำตั้งแต่ 256 กิโลไบ
ขึ้นไป และใช้ระบบการจัดการของดอ
เวอร์ชัน 2.0 ขึ้นไป สามารถทำงานไ
ทั้งบนพีซีและในระบบแลน

การทำงานของ VIRUSCAN8
สามารถแบ่งการทำงานได้เป็น 3 ลักษณ
คือ

1. SCAN, NETSCAN ใช้ในกา
ตรวจค้นหาไวรัส
2. CLEAN ใช้ในการทำลายไวรั
3. การทำงานในส่วนของ VSH
ELD

SCAN

VIRUSCAN82 สามารถที่จะ
SCAN หาไวรัสใน NET WORK DRIVI
ในระบบ LAN ได้ นอกจากนั้นแล้วไฟล์
ต่าง ๆ ที่ถูกบีบข้อมูลด้วยโปรแกรมบีบ
ข้อมูล เช่น PKZIP โปรแกรม VIRU
SCAN82 ก็สามารถเข้าไปตรวจเช็คหา
ไวรัสได้ ซึ่งจะมีพารามิเตอร์ที่น่าสนใจ
ที่จะใช้งานร่วมกับคำสั่ง SCAN ดังนี้

\	ให้ SCAN หาไฟล์ในราก ไดเรคทอรี และบูตเซกเตอร์ ต่าง ๆ
/A	SCAN หาไฟล์ทุก ๆ ไฟล์
/AV	สร้าง Validation code ใน

ไฟล์ ไฟล์จะมีขนาดเพิ่มขึ้น 10 กิโลไบต์

/CHKHI เช็คหน่วยความจำตั้งแต่ 0 กิโลไบต์ ถึง 1088 กิโลไบต์

/CV ตรวจสอบหา Vaidation code ว่ามีการเปลี่ยนแปลงของไฟล์หรือไม่

/D ลบไฟล์ที่ติดไวรัสออก

/E .XXX .YYY .ZZZ สแกนหา overlay ของไฟล์ที่มีนามสกุลต่าง ๆ ตามที่กำหนดไว้

/FR แสดงข้อความที่เป็นภาษาฝรั่งเศส

/M สแกนหาไวรัสในหน่วยความจำทั้งหมด

/MAINT ใช้ในการสแกนหาไวรัสในฮาร์ดดิสค์ที่ทำการ INSTALL ด้วย DOS 4.0

/EXT d: filename สแกนหาโปรแกรมที่เป็นเท็กซ์ไฟล์ (Text file)

/MANY ใช้ในการสแกนหาไวรัสในดิสเกตต์ทีละหลาย ๆ แผ่น โดยไม่ต้องเรียกโปรแกรมซ้ำกันหลาย ๆ ครั้ง

/NOMEM ใช้ในกรณีที่ไม่ต้องการตรวจเช็คหน่วยความจำ เมื่อแน่ใจว่าในระบบปฏิบัติงานปราศจากไวรัส

/RV ลบ Validation Code ออกจากไฟล์

/SUB สแกนหาไวรัสในซับไดเรคทอรี

จากพารามิเตอร์ที่กล่าวมาทั้งหมดนี้ สามารถเรียกใช้งานพร้อมกันได้ เช่น

SCAN d1...d110 : /A/AV/CHKHI/CV/D/E
/XXX .YYY .ZZ /EXT d:filename/FR
/INT/MANY/NIZ/MPBREAK/NOMEM
/NOPAUSE/REPORT d:filename
/RV/SUB

สิ่งแปลกใหม่

VIRUSCAN82 ได้พัฒนาตัวเองและเพิ่มประสิทธิภาพการทำงานให้มากขึ้น ได้แก่

– สามารถที่จะตรวจสอบไวรัสได้มากขึ้นกว่าเวอร์ชันเดิม

– ได้เพิ่มพารามิเตอร์ในการใช้งานร่วมกับคำสั่ง SCAN เพื่อให้สามารถทำงานได้มากขึ้น ดังต่อไปนี้

/CHKHI

ใช้สำหรับสแกนหาไวรัสในหน่วยความจำ ปกติแล้วโปรแกรม VIRUSCAN82 จะสามารถตรวจค้นหาไวรัสในหน่วยความจำได้เพียง 640 กิโลไบต์ ถ้ามีหน่วยความจำที่เกินจาก 640 กิโลไบต์ เช่น การ extended memory โปรแกรม VIRUSCAN ในเวอร์ชันเดิมไม่สามารถตรวจเช็คเข้าไปถึงส่วนนั้นได้ แต่ VIRUSCAN82 ได้เพิ่มพารามิเตอร์ /CHKHI เพื่อช่วยในการตรวจเช็คหน่วยความจำในส่วนที่เกินมา ซึ่งสามารถที่จะทำการตรวจเช็คตั้งแต่หน่วยความจำที่มีขนาด 0 กิโลไบต์ ถึง 1088 กิโลไบต์

/MAINT

ใช้สำหรับสแกนหาไวรัสในส่วนของฮาร์ดดิสค์ที่ใช้ระบบการจัดการด้วย DOS 4.0 หรือในกรณีที่ต้องการตรวจสอบว่าบูตเซกเตอร์และตารางพาร์ติชันได้รับอันตรายจากไวรัสหรือไม่ ถ้าหากในส่วนนั้นได้รับอันตรายจากไวรัส จะแสดงข้อความบนจอภาพว่า "INVALITAD MEDIA" เมื่อเกิดขึ้นในกรณีนี้ฮาร์ดดิสค์จะไม่สามารถอ่านและใช้งานข้อมูลเหล่านั้นได้ /MAINT จะช่วยในการสแกนหาไวรัสในส่วนบูตเซกเตอร์และตารางพาร์ติชันพร้อมทั้งช่วยกู้ไฟล์ข้อมูล

เหล่านั้นจากไวรัส

3. เพิ่มข้อมูลต่าง ๆ ที่เกี่ยวกับไวรัสคอมพิวเตอร์อีก 49 ชนิด เช่น the dec 28, Miky, the Sunday-2, 1014, 2480, Noback, Topo, Tuesday, Twin-351, Mini-45 Mule, Newcom เป็นต้น

CLEAN

เป็นโปรแกรมที่ใช้ในการกู้ข้อมูลที่ติดไวรัสกลับคืนมา โดยมีรูปแบบการใช้งานดังนี้

CLEAN d1...d10 : [VIRUS ID] (ชื่อย่อของไวรัส)

พารามิเตอร์ที่กำหนดคำสั่งที่ใช้งานจะเป็นตัวเดียวกันกับ SCAN โปรแกรม CLEAN สามารถแก้ไขไวรัสได้ทีละหนึ่งตัวเท่านั้น

VSHIELD

โปรแกรมที่ช่วยในการป้องกันไวรัสไม่ให้เข้าสู่ระบบการทำงาน เมื่อทำการรันโปรแกรม VSHIELD จะทำการตรวจเช็คหาไวรัสในส่วนต่าง ๆ ที่สำคัญเสียก่อน เช่น หน่วยความจำ บูตเซกเตอร์ ตารางพาร์ติชัน command.-

com เมื่อพบว่าปราศจากไวรัสก็จะทำการเรสซิเดนต์โปรแกรมลงในหน่วยความจำเพื่อทำการป้องกันไวรัส โดยจะเข้าไปดักการทำงานของดอสไว้ จึงขอแนะนำให้เขียนไว้ใน Autoexec.Bat เพื่อสะดวกในการทำงาน ลักษณะการทำงานของ VSHIELD จะเป็นแบบโปรเทคชัน (Protection)

การเพิ่ม Signature

ในโปรแกรมนี้ สามารถจะเพิ่ม Signature ของไวรัสที่โปรแกรมไม่รู้จักเข้าไปได้ โดยเข้าไปเก็บไว้ในไฟล์และใช้ /EXT เป็นตัวช่วยในการอ่านไฟล์ขึ้นมาใช้งาน ในการสร้าง Signature ของไวรัส มีรูปแบบการใช้งานดังนี้

```
# เขียนคำอธิบายเกี่ยวกับไวรัสคอมพิวเตอร์ ชนิดที่ 1
  "aabbccddeeff" ชื่อของไวรัสชนิดที่ 1
# เขียนคำอธิบายเกี่ยวกับไวรัสคอมพิวเตอร์ ชนิดที่ 2
  "gglliijjkk.." ชื่อของไวรัสชนิดที่ 2
.
.
.
"nnvvwwxxyyzz" ชื่อของไวรัสชนิดที่ n
```

โดยค่าใน aa, bb, cc และอื่น ๆ จะต้องกำหนดให้เป็นเลขฐานสิบหกเป็นข้อมูลที่เกี่ยวกับไวรัสคอมพิวเตอร์ ซึ่งเป็นข้อมูลเฉพาะของไวรัสที่ใช้ในการสแกนหา

การสร้างไฟล์

สามารถที่จะสร้างไฟล์ที่เป็น Signature ของไวรัส โดยการใช้โปรแกรม Editor หรือเวิร์ดโปรเซสเซอร์และเก็บไว้ในไฟล์เท็กซ์ เช่น จะสร้างไฟล์ที่เก็บ Signature ของไวรัสคอมพิวเตอร์ ดังนี้

```
# Sing a Song, Create FROM Thai
"B8 01 03 89 0E 20 7C 88 36 22 70"
Lao Duang Duen
```

แล้วทำการเซฟเก็บไว้ในชื่อไฟล์ที่ต้องการ สมมติให้ไฟล์ชื่อ THAI.TXT

สามารถที่จะ SCAN หาไวรัสนี้ได้ โดยใช้คำสั่ง

```
A> SCAN A: /EXT A:THAI.TXT
```

เมื่อโปรแกรมทำงานก็จะทำการตรวจหาไวรัสที่เพิ่มเข้ามาให้ด้วย การเพิ่ม Signature ของไวรัสชนิดใดก็ตาม ผู้ที่ทำการเพิ่มเข้าไปควรรู้จัก Signature ของไวรัสตัวนั้นเป็นอย่างดีเสียก่อน เพื่อป้องกันการตรวจเช็คและค้นหาข้อผิดพลาด

VIREX-PC

Virex-PC เป็นโปรแกรมแอนตี้ไวรัสอีกตัวหนึ่งที่มีความสามารถไม่แพ้ 2 ตัวแรกที่กล่าวไปแล้ว Virex-PC สามารถทำงานบนเครื่อง IBM PC/XT, PC/AT, PS/2 และ LAN การทำงานของ Virex-PC จะเป็นทั้ง Detection และ Removal Virus สามารถตรวจสอบหาไวรัสได้ 50 ชนิด และใช้เนื้อที่ในหน่วยความจำ 30 เมกะไบต์

การติดตั้งระบบ

ก่อนทำการติดตั้งระบบควรใช้โปรแกรม VPCSCAN.EXE ตรวจสอบระบบงานก่อนว่ามีไวรัสหรือไม่ ถ้าไม่มีไวรัสในระบบก็สามารถทำการติดตั้งระบบได้ โดยใช้คำสั่ง install ที่อยู่ในแผ่นซอฟต์แวร์ ถ้าพบว่ามีไวรัสโปรแกรม VPCSCAN จะมีออปชันให้เลือก เพื่อใช้ในการทำงานรูปที่ 5

นอกจากความสามารถในการกู้ไฟล์ข้อมูลจากไวรัสคอมพิวเตอร์แล้ว Virex-PC ยังสามารถทำการโปรเทคชันไฟล์ข้อมูลต่าง ๆ ที่มีอยู่ โดยจะทำการโปรเทคชันไฟล์เหล่านั้นไปเก็บไว้ในส่วนพาร์ติชัน ซึ่งจะทำการเก็บไว้ในไฟล์ VIREXPC.DAT

วิธีการ INSTALL

ให้นำแผ่น Virex-PC ใส่ลงไปในไดรฟ์ A: แล้วเรียกโปรแกรม Install จากแผ่นดิสค์

```
A> INSTALL <ENTER>
```

จะมีข้อความแสดงบนจอ ซึ่งเป็นออปชันให้เลือกดังรูปที่ 6

ให้เลือกว่าต้องการจะให้พาสเวิร์ดหรือไม่ ถ้าไม่ต้องการให้กด I เมื่อกด I แล้วที่หน้าจอจะแสดงข้อความเพื่อให้ตอบคำถามดังนี้

```
1) On what drive would you like to insta
Virex-PC [C:]?
```

ถ้าต้องการให้ INSTALL โปรแกรม Virex-PC ลงไปที่ไดรฟ์ C: ให้

```
– attempt to remove the virus form the original file
(if VPCScan knows how to disinfect files infected by this particular virus)
– erase this the infected file
– leave the file as is
```

รูปที่ 5 แสดงออปชันให้เลือก เมื่อมีการตรวจเช็คโปรแกรมแล้วพบว่ามีไวรัสอยู่ในระบบ

กด Enter แต่ถ้าต้องการ INSTALL ลงในไดรฟ์อื่น ๆ ให้ป้อนตัวอักษรตามไดรฟ์ที่ต้องการ

2) In what directory on <drive> would you like to install Virex-PC [/]?

ถ้าต้องการที่จะให้ INSTALL ลงซับไดเรคทอรีใดให้พิมพ์ชื่อไดเรคทอรีลงไป

3) What name would you like to give your protection file [Virex-PC.DAT]?

ถ้าต้องการให้เก็บรายชื่อไฟล์ที่โปรเทคชันไว้ในชื่อ Virex-PC ให้กด Enter แต่ถ้าต้องการเก็บไว้ในชื่ออื่นให้พิมพ์เข้าไป

4) What name would you like to give the Virex-PC program [Virex-PC.COM]?

ถ้าต้องการให้โปรแกรม Virex-PC เก็บไว้ในไฟล์ชื่อ VirexPC.COM หรือไม่ ถ้าต้องการให้กด Enter แต่ถ้าไม่ต้องการให้พิมพ์ชื่อและนามสกุลไฟล์ที่จะเก็บลงไป

5) Would you like Virex-PC to run each time you boot your sysetm [Y]?

ถ้าต้องการให้โปรแกรม Virex-PC รันในขณะที่ทำการบูตเครื่องให้กด Y โปรแกรมจะเข้าไปแก้ไขไฟล์ Autoexec.-Bat ทันที แต่ถ้าไม่ต้องการให้รันในขณะบูตเครื่องให้ตอบ N เมื่อตอบ N แล้วโปรแกรมจะให้แสดงข้อความดังรูปที่ 7

ถ้ากด Enter หรือ Y จะทำการเซตค่าในการโปรเทคชันในไฟล์ให้ซึ่งจะมีคำถามแสดงบนจอภาพให้คุณตอบคำถามตามต้องการ

ถ้ากด M จะใช้ในกรณีที่ต้องการใส่พาสเวิร์ดให้กับระบบงาน ส่วนมากจะนิยมใช้เมื่อมีผู้ใช้งานร่วมกันหลายคน โดยแต่ละคนจะมีพาสเวิร์ดของตัวเอง เมื่อกด M แล้วจะมีข้อความแสดงบนจอภาพดังนี้

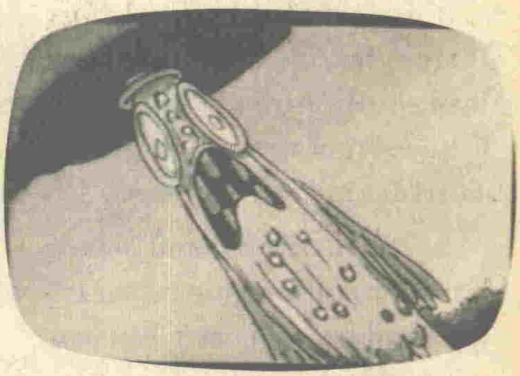
Enter the member of the user file you wish to edit, 'A' to add, 'D' to delete or <CR> to save changes and return to Dos:

โปรแกรมจะให้ป้อนจำนวนผู้ใช้งานในระบบงานว่ามีกี่คน เมื่อป้อนจำนวนเลขเข้าไปแล้วให้กด Enter ที่จอภาพจะแสดงข้อความให้ป้อนชื่อและพาสเวิร์ดของผู้ใช้งานแต่ละคน ถ้าต้องการจะเพิ่มจำนวนผู้ใช้งานให้กด 'A' แล้วกด Enter ถ้าต้องการลบชื่อผู้ใช้งานในระบบออกให้กด 'D' แล้วกด Enter โปรแกรมจะทำการแก้ไขรูทีนเหล่านั้นให้

เมื่อทำการสร้างพาสเวิร์ดให้กับระบบ โปรแกรม Virex-PC จะสร้างไฟล์ Virexpc.PSW เพื่อเก็บพาสเวิร์ดของผู้ใช้แต่ละคน

วิธีการใช้งาน

เมื่อทำการติดตั้งโปรแกรมเรียบร้อยแล้ว ให้ทำการบูตเครื่องใหม่ โดยกด CTRL-ALT-DEL สามารถทำการรันโปรแกรม โดยใช้



A>VPCSCAN <drive> [ENTER]

เมื่อกด ENTER แล้วจะมีข้อความแสดงหน้าจอ ดังรูปที่ 8

กด Y โปรแกรมจะทำการตรวจเช็คหาไวรัสให้ ถ้ากดคีย์ใด ๆ จะยกเลิกการทำงานทันที การทำงานของ Virex-PC จะมีการป้องกันตลอดเวลา โดยจะมีข้อความต่าง ๆ เตือน เช่น

Install and Maintain Virex-PC (No Password) (Press 'I')
Modify User Files (Password Protected) (Press 'M')
Which would you like to do

รูปที่ 6 แสดงข้อความแนะนำเมื่อทำการ INSTALL โปรแกรม

Your Protection File be called : <your protection file name>
The Virex-PC program will be called : <your program file name>
Virex-PC will (will not) be run each time you start your computer OK?

รูปที่ 7

You are attempting to run an unregisterd program named:
C:\ VPC SCAN.EXE
Doing so *might* introduce a virus to your system.
Enter 'Y' to run the program or any other key to abort it.

รูปที่ 8

ถ้าทำการเรียกไฟล์บางไฟล์มาใช้งาน โดยเรียกโปรแกรมผ่านจากไดรฟ์ A: หรือไดรฟ์อื่น ๆ ที่ไม่ใช่ไดรฟ์ที่ Virex-PC ทำการโปรเทคชันไว้ จะแสดงข้อความเตือน ดังรูปที่ 9

ถ้าต้องการทำการก๊อบปี้ไฟล์จากไดรฟ์ที่ทำการโปรเทคชันโดย Virex-PC ไปยังไดรฟ์ต่าง ๆ ที่ต้องการ โปรแกรมจะแสดงข้อความดังรูปที่ 10

ถ้ากด Y โปรแกรมยังแสดงข้อความเตือนอยู่ แต่ถ้า G โปรแกรมจะทำการก๊อบปี้ไฟล์ต่าง ๆ ให้ตามต้องการ และกดคีย์ใด ๆ โปรแกรมจะยกเลิกการทำงานทันที

CPAV และ NAV

สำหรับโปรแกรม CPAV (CENTRAL POINT ANTIVIRUS) สามารถอ่านรายละเอียดการทำงานและการใช้งานต่าง ๆ ของโปรแกรมในคอลัมน์รีวิว ฉบับที่ 79 และ NAV (NORTON ANTIVIRUS) สามารถอ่านรายละเอียดการทำงานได้จากคอลัมน์รีวิวในหนังสือไมโครคอมพิวเตอร์ฉบับที่ 69

ประกาศศักดา

จากบทความนี้ได้ทำการเปรียบเทียบการทำงานต่าง ๆ ของโปรแกรมตรวจสอบไวรัสได้ดังตารางที่ 1 จากตารางที่ 1 คงช่วยให้ผู้อ่านสามารถที่จะตัดสินใจในการเลือกแอนตี้ไวรัสแต่ละตัวเพื่อช่วยป้องกันอันตรายให้กับระบบงานของคุณ

สรุป

โปรแกรมแอนตี้ไวรัสแต่ละตัวก็มีความสามารถในการป้องกันไวรัสที่แตกต่างกันออกไปแสดงดังตาราง 2, 3 และ 4, 5, 6

```
You are attempting to run an unregistered program named:
C: \ VTILS \ SCAN.EXE
Doing so might introduce a virus to your system Enter
'Y' to run the program, or any other key to abort it.
```

รูปที่ 9 แสดงข้อความเตือนในขณะที่เรียกใช้งานในไฟล์ต่าง ๆ

```
Attem to open a file with write Access begin made on :
B: \ SCAN \ SCAN.EXE
(By the Command line Interpreter)
Press "Y" to allow, "G" to go till exit, any other key to exit.
```

รูปที่ 10 แสดงข้อความเตือนในขณะที่ต้องการก๊อบปี้ไฟล์

ความสามารถในการทำงาน	N	Y	N	Y	Y
	VirusCure	VirusCAN82	Virex-PC	CPAV	NAV
Chacksum	Y	Y	Y	Y	Y
Signature Chacking	Y	Y	Y	Y	Y
Protects boot Sector	Y	Y	Y	Y	Y
Protect command.com	Y	Y	Y	Y	Y
Protect FAT	Y	Y	Y	Y	Y
Protect patition file	Y	Y	Y	Y	Y
Protect RAM	Y	Y	Y	Y	Y
Program For WINDOWS	N	Y	N	Y	Y
LAN	Y	Y	Y	Y	Y
Add Virus	Y	Y	N	Y	Y

Y = สามารถทำงานได้
N = ไม่สามารถทำงานได้

ตารางที่ 1 เปรียบเทียบการทำงานต่าง ๆ ของโปรแกรมแอนตี้ไวรัส

VIRUSCURE PLUS

	DARK AVENGER	JOSHI	RED CROSS	JERUSALEM
DETECTION	PA	PA	NP	PA
REMOVAL	PA	PA	NP	PA
PROTECTION	PA	PA	NP	PA

PA = โปรแกรมสามารถตรวจเช็คได้
NP = โปรแกรมไม่สามารถตรวจเช็คได้

ตารางที่ 2 แสดงความสามารถในการป้องกันไวรัสของโปรแกรม VIRUSCURE PLUS

ป้องกันอย่างไร

ผู้เชี่ยวชาญเกี่ยวกับไวรัสคอมพิวเตอร์ได้เสนอข้อแนะนำในการรักษาความปลอดภัยของข้อมูลและการป้องกันไวรัสไว้ทั้งหมด 8 วิธีโดยสังเขป

1. ถ้าต้องการบูตดอสจากแผ่นดิสเกตต์ ควรทำการตรวจเช็คดิสเกตเสียก่อนว่ามีไวรัสหรือไม่ ถ้าปราศจากไวรัสให้ติด WRITE-PROTECT ไว้และ

VIRUSCAN82

	DARK AVENGER	JOSHI	RED CROSS	JERUSALEM
DETECTION	PA	PA	PA	PA
REMOVAL	PA	PA	PA	PA
PROTECTION	PA	PA	PA	PA

PA = โปรแกรมสามารถตรวจเช็คได้
NP = โปรแกรมไม่สามารถตรวจเช็คได้

ตารางที่ 3 แสดงความสามารถในการป้องกันไวรัสของโปรแกรม VIRUSCAN82

VIREX-PC

	DARK AVENGER	JOSHI	RED CROSS	JERUSALEM
DETECTION	PA	PA	PA	PA
REMOVAL	PA	NP	NP	PA
PROTECTION	PA	NP	NP	PA

PA = โปรแกรมสามารถตรวจเช็คได้
NP = โปรแกรมไม่สามารถตรวจเช็คได้

ตารางที่ 4 แสดงความสามารถในการป้องกันไวรัสของโปรแกรม VIREX-PC

NAV

	DARK AVENGER	JOSHI	RED CROSS	JERUSALEM
DETECTION	PA	PA	NP	PA
REMOVAL	PA	PA	NP	PA
PROTECTION	PA	PA	PA	PA

PA = โปรแกรมสามารถตรวจเช็คได้
NP = โปรแกรมไม่สามารถตรวจเช็คได้

ตารางที่ 5 แสดงความสามารถในการป้องกันไวรัสของโปรแกรม NAV

CPAV

	DARK AVENGER	JOSHI	RED CROSS	JERUSALEM
DETECTION	PA	PA	PA	PA
REMOVAL	PA	PA	PA	PA
PROTECTION	PA	PA	PA	PA

PA = โปรแกรมสามารถตรวจเช็คได้
NP = โปรแกรมไม่สามารถตรวจเช็คได้

ตารางที่ 6 แสดงความสามารถในการป้องกันไวรัสของโปรแกรม CPAV

ใช้แผ่นนั้นเป็นแผ่นบูตตลอด

2. ควรตรวจสอบแผ่นซอฟต์แวร์ตัวใหม่ทุกครั้ง ก่อนทำการ install ลงฮาร์ดดิสก์ เพื่อป้องกันไวรัสที่อยู่ในแผ่นติดลงไปในฮาร์ดดิสก์

3. ติด WRITE-PROTECT บนดิสก์เสียก่อน ในขณะที่มีการใช้งานบนเครื่องพีซี ถ้าต้องการที่จะนำซอฟต์แวร์ตัวใหม่เข้าไปทำงานหรือติดตั้งในระบบ (INSTALL) ก่อนที่จะทำการติดตั้งซอฟต์แวร์ควรทำการติด WRITE-PROTECT ไปบนแผ่นซอฟต์แวร์นั้นเสียก่อน เพื่อป้องกันอันตรายจากไวรัสในหน่วยความจำ (ถ้ามี) ติดลงไปบนแผ่นซอฟต์แวร์ตัวใหม่ ในอีกกรณีหนึ่งคือ ไม่ควรทำ reset เครื่องใหม่ (Ctrl-Del Alt) ในขณะที่แผ่นซอฟต์แวร์ตัวใหม่อยู่ในไดรฟ์ A: เพราะอาจทำให้ไวรัสที่อยู่ในหน่วยความจำลงไปบนแผ่นซอฟต์แวร์ตัวใหม่ หรือไวรัสที่อยู่ในแผ่นซอฟต์แวร์ติดลงไปยังความจำบนพีซีหรือฮาร์ดดิสก์ได้

4. หมั่นตรวจสอบฮาร์ดดิสก์ที่ใช้งานบ่อย ๆ และควรนำไฟล์แอนตี้ไวรัสเขียนลงไปใน AUTOEXEC.BAT เพื่อจะเรียกใช้งานในขณะทำการเปิดเครื่อง

แอนตี้ไวรัสจะทำการตรวจสอบภายในระบบและไฟล์ทุกไฟล์ ซึ่งทำให้มีความมั่นใจว่าภายในระบบปราศจากไวรัส

5. หมั่นตรวจสอบหา BAD SECTOR ในฮาร์ดดิสก์ เพราะมีไวรัสบางตัวที่เข้าไปทำการมาร์คส่วนของเซกเตอร์บางเซกเตอร์ให้เป็น BAD SECTOR ซึ่งจะทำให้เกิดอันตรายกับข้อมูลเป็นอย่างมาก

6. เปลี่ยนแอตทริบิวต์ไฟล์ที่สำคัญให้เป็น read-only วิธีการนี้เป็นวิธีการที่ดีที่สุดและสามารถป้องกันไวรัสได้ผล 100% พร้อมทั้งสามารถป้องกันไวรัสในระบบ network ได้อีกด้วย การเปลี่ยนแอตทริบิวต์ของไฟล์ให้เป็น read-only สามารถใช้คำสั่งจากดอสได้ โดยใช้คำสั่ง ATTRIB หรือจะใช้โปรแกรมยูทิลิตี้ทั้งหลายช่วยในการเปลี่ยนก็ได้ เช่น PCTOOLS, NORTON UTILITY

7. ไวรัสที่ติดตรงตำแหน่งบูตเซกเตอร์นั้น สามารถที่จะติดไฟล์ได้ง่ายที่สุด โดยเฉพาะถ้าเกิดขึ้นในระบบเน็ตเวอร์กอาจก่อความเสียหายให้กับข้อมูลเป็นอย่างมาก ดังนั้นเพื่อป้องกันไม่ให้ไวรัสติดในส่วนของบูตเซกเตอร์ไม่ควรทำการบูตแผ่นจากไดรฟ์ A: และไม่ควรทำการถ่ายข้อมูล โดยผ่านเครื่องคือถ่ายข้อมูลโดยวิธีการก๊อบปี้ เนื่องจากวิธีการก๊อบปี้นั้นจะต้องทำการก๊อบปี้บูตเซกเตอร์ไปด้วย ดังนั้นถ้าต้องการถ่ายข้อมูลควรถ่ายข้อมูลผ่านระบบเน็ตเวอร์ก โดยอาศัยโมเด็ม เพราะจะทำให้ได้ข้อมูลที่ถูกต้องและสมบูรณ์ที่สุดและยังปราศจากไวรัสบูตเซกเตอร์อีกด้วย

8. วิธีสุดท้าย เป็นวิธีที่นิยมกันทำกันมานานแล้ว เนื่องจากเป็นวิธีที่ง่ายและปลอดภัย คือการสำรองข้อมูล (Back-up Data) ไว้อีก 1 ชุด เมื่อมีการอัพเดตข้อมูลทุกครั้งควรทำการสำรองข้อมูลไว้

ของฝากก่อนจาก

จากบทความทั้งหมดคงจะพอให้คุณตัดสินใจได้แล้วนะคะว่าจะใช้งานแอนตี้ไวรัสตัวไหนดี ก่อนจากกันวันนี้ดิฉันจะขอฝากไวรัสน้องใหม่ (ตัวไวรัส) อีกตัวหนึ่ง เพื่อให้คุณได้รู้จัก ไวรัสตัวนี้ชื่อ "GP1"

"GP1" เป็นไวรัสใหม่ล่าสุดที่ถูกค้นพบและเป็นไวรัสเพียงชนิดเดียวที่ถูกค้นพบ ความแตกต่างระหว่างไวรัสในเครื่องพีซีทั่ว ๆ ไปกับไวรัสที่เกิดขึ้นในระบบ LAN ก็คือ มันถูกออกแบบมาเป็นพิเศษเพื่อให้ไปโจมตีการทำงานของ FILE SERVER ไวรัสชนิดนี้เป็นการแปรสภาพไวรัสเยรูซาเล็ม (JERUSALEM VIRUS) ซึ่งถูกสร้างขึ้นเพื่อจุดประสงค์พิเศษคือ เพื่อให้เจาะเข้าไปในระบบความปลอดภัยของโนเวลล์และแพร่กระจายเข้าไปในระบบเน็ตเวอร์ก ซึ่งแม้ว่าผู้ใช้จะเปิดเครื่องก็ใช้งานได้น้อยที่สุด

แม้ว่า "GP1" จะถูกออกแบบเพื่อให้เข้าไปทำลายโนเวลล์ไฟล์ เซอร์ฟเวอร์ แต่ก็ยังมีข้อจำกัดอยู่บ้างสำหรับการออกแบบชนิดนี้ คือ มันจะติดต่อไปยังไฟล์อื่น ๆ เพียง IPX.COM ถูกติดตั้งแล้วเท่านั้น ไวรัสในระบบ LAN ชนิดนี้ จะไม่ใช้ดอสเพื่อสลายตัวเอง ซึ่งไม่เหมือนกับไวรัสธรรมดาทั่ว ๆ ไป "GP1" ต้องคอยให้ NOVELL TSR PROGRAMS ถูกติดตั้งเสียก่อน (IPX and NET) เพื่อให้สามารถเริ่มต้นหน้าที่ MONITORING ของ 21h (ถูกจัดโดย The Netware Kernel) และสลายตัวเองครั้นเมื่อ Novell TSR Programs เหล่านี้ถูกติดตั้งเรียบร้อยแล้ว ไวรัส "GP1" ก็ยังสามารถเข้าไปละเมิดสิทธิการใช้งานของผู้ใช้และเข้าถึงแหล่งข้อมูล ซึ่งโดยปกติแล้วจะไม่สามารถเข้าไปถึงได้

หลังจากการวิเคราะห์ "GP1" แล้ว ทางวิศวกรของ Trend ก็พบหลายสิ่งหลายอย่างที่เป็นบุคลิกที่น่าสนใจมาก ๆ ของไวรัสในระบบ LAN ตัวนี้ ข้อแรกก็คือ "GP1" เริ่มเข้าไปในจุดต่าง ๆ ซึ่งขึ้นอยู่กับว่า มันจะติดเชื้อจาก .EXE and .COM files ดังนั้นความยาวของไวรัสจะแตกต่างกันใน .COM and .EXE files "GP1" ไม่ได้อยู่ในระบบการทำงานของทั้ง .EXE and .COM files การจะใช้งานของพวกมันก็เพียงการ INSTALL หรือเคลื่อนย้ายจากเมมโมรีเท่านั้น ถ้าไวรัสนี้อยู่ในเมมโมรีและถ้าอักษรตัวแรกในคำสั่งไม่ใช่ตัวอักษร "I" "GP1" จะเคลื่อนย้ายตัวมันเองจากเมมโมรีและข้อมูล จะปรากฏบนจอว่า "GP1 Removed From Memory" สำหรับรายละเอียดของไวรัส "GP1" ได้รับความเอื้อเฟื้อจากบริษัทซีบร้า คอมพิวเตอร์ที่ได้จัดส่งเอกสารมาให้ ขอขอบคุณมา ณ โอกาสนี้ด้วย สวัสดีค่ะ